UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,094	02/17/2004	Duc Pham	AESN3016	9897

23488 7590 03/14/2008

GERALD B ROSENBERG
NEW TECH LAW
260 SHERIDAN AVENUE
SUITE 208
PALO ALTO, CA 94306-2009

EXAMINER	
SCHMIDT, KARI L	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
03/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,094	PHAM ET AL.	
	Examiner	Art Unit	
	KARI L. SCHMIDT	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: Figure 9C is not shown in "Brief Description of the Drawings".

The examiner notes the applicant is suggested to add Figure 9C and provide a brief description of the drawings listed in section "Brief Description of the Drawings".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-42 are rejected under 35 U.S.C. 102(b) as being anticipated by Tumblin et al. (US 6,490,679 B1).

Claim 1

Tumblin discloses a security server that operates to conditionally enable establishment of a secure interprocess communications session between designated application program instances, said security server comprising (see at least, col. 5, lines 14-34: the examiner notes client programs and server programs as application instances and col. 5, line 58 – col. 6, line 13: the examiner notes a security integration server which is

connected to a network and further the examiner notes that the client or server transmit policy requests to the policy server program on the security integration server and FIG. 2 and 9 the examiner notes the security server of FIG. 9 is attached to the same network 110 as the programs of the client/server program of FIG. 2): a) a policy database storing a plurality of policy rules that collectively define the mutual authentication and authorization requirements for establishing a interprocess communications session between first and second application instances (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs (col. 5, lines 14-34) via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program); and b) a security controller interoperative with an operating system that includes an application call interface (see at least, column 6, lines 14-24: the examiner notes a security service API) operative to enable establishment of said interprocess communications session (see at least, col. 6, lines 14-24), said security controller being operative to receive predetermined authentication and authorization information from said operating system (see at least, 5, lines 34-41: the examiner notes the use of SIM API for the client and server ASIM and NSIM) in connection with a predetermined application call request to establish said interprocess communications session (see at least, col. 5, lines 34-51: the examiner notes both the ASIM and NSIM are linked to the SIM which provide security provider

interface to said security integration server), said security controller (e.g. SIM, see at least, col. 5, lines 52-58) being further operative to evaluate said predetermined application call request and said predetermined authentication and authorization information against said plurality of policy rules to conditionally permit the establishment of said interprocess communications session with respect to said first and second application instances (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs (col. 5, lines 14-34) via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program).

Claim 2

Tumblin discloses the security server of claim 1 wherein said security controller is operative to establish a session key that defines a unique encryption of communications data transferred through said communications session between said first and second application instances (col. 9, lines 32-37: the examiner notes the use of session key for pre-established communication is based on a new session token which is unique for each client and server program communication).

Claim 3

Tumblin discloses the security server of claim 2 wherein said security controller is operative to evaluate said predetermined application call request and said predetermined authentication and authorization information against said plurality of policy rules to selectively control establishment of said session key with respect to said first and second application instances (see at least, col. 5, lines 58 – col. 6, line 9 and col. 7, lines 36-65: the examiner notes the use of creating a session between requesting programs based on the policy server program and policy information for each program and col. 9, lines 32-37:the examiner notes the use of session key for pre-established communication is based on a new session token which is unique for each client and server program communication).

Claim 4

Tumblin discloses the security server of claim 3 wherein said security controller is operative to provide said session key to said operating system to enable said unique encryption communications data (col. 9, lines 32-37: the examiner notes the use of session key for pre-established communication is based on a new session token which is unique for each client and server program communication).

Claim 5

Tumblin disclose the security server of claim 4 wherein said first and second application instances are executed on a common host computer system (see at least, col. 2, lines 36-46 and FIG. 1 and FIG. 2; the examiner notes plurality of programs per host entity) .

Claim 6

Tumblin discloses the security server of claim 1 wherein said security server is coupleable to said operating system through a network communications connection (see at least, col. 5, line 58 – col. 6, line 9).

Claim 7

Tumblin discloses an interprocess communications security system enabling secure communications sessions to be established between designated application instances, said interprocess communications security system comprising (see at least, abstract and col. 6, lines 14-24: the examiner notes the client program on the client seeks to open a secure communications channel with a server program on a server): a) a first computer system coupleable to a communications network, wherein said first computer system includes a first operating system operative to support execution of a first application instance by said first computer system, said first operating system including a first policy enforcement module operative to qualify predetermined communications calls made between said first application instance and said first operating system (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information

regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the client program on the client); b) a second computer system coupleable to a communications network, wherein said second computer system includes a second operating system operative to support execution of a second application instance by said second computer system, said second operating system including a second policy enforcement module operative to qualify predetermined communications calls made between said second application instance and said second operating system (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the server program on the server); and c) a security appliance coupleable to said first and second computer systems through said communications network, said security appliance being interoperable with said first and second policy enforcement modules to mutually authenticate said first and second application instances to conditionally conduct interprocess communications (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program)).

Claim 8

Tumblin discloses the interprocess communications security system of claim 7 wherein said security appliance is further interoperable with said first and second policy enforcement modules to enable encryption processing of interprocess communications exchanged between said first and second application instances (col. 5, line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 9, lines 32-37: the examiner notes the use of a session key for secure communication between the client and server program).

Claim 9

Tumblin discloses the interprocess communications security system of claim 8 wherein said security appliance is operative to determine an encryption token with respect to the mutual authentication of said first and second application instances, to provide said encryption token to said first and second policy enforcement modules for use in encrypting processing of interprocess communications exchanged between said first and second application instances (see at least, col. 6, lines 42-47: the examiner notes the use of a session token between the client and server program before the use of an encrypted session key for secure communication).

Claim 10

Tumblin discloses the interprocess communications security system of claim 9 wherein said security appliance includes a policy database storing a plurality of policy rules (see at least, col. 5, line 58 – col. 6, line 9) and a control program operative to evaluate said plurality of policy rules (see at least, col. 5, line 58 – col. 6, line 9: the examiner notes a policy server program), wherein said first and second policy enforcement modules are operative to provide said security appliance with predetermined information associated with said first and second application instances in connection with a predetermined communications call request by said first application instance to establish interprocess communications with said second application instance, and wherein said security appliance conditionally enables establishment of an interprocess communications session between said first and second application programs in response to said predetermined communications call request dependent on an evaluation of said plurality of policy rules with respect to said predetermined information (see at least, col. 5, line 58 – col. 6, line 9: the examiner notes the use of program policies and connection policies that govern the first and second policy enforcement and the predetermined secure communication session).

Claim 11

Tumblin discloses the interprocess communications security system of claim 10 wherein said predetermined information includes a secure identification of said first and second application instances and wherein said secure identification is used to mutually

authenticate said first and second application instances (see at least, col. 5, lines 51-57: the examiner notes that each SPIM is linked to an SKI which is used as a secure identification for both client and server program).

Claim 12

Tumblin discloses the interprocess communications security system of claim 11 wherein said security appliance includes a signature database storing a plurality of secure signatures, wherein said predetermined information includes secure signatures for said first and second application instances, and wherein said security appliance is operative to compare the secure signatures of said first and second application instances to said plurality of secure signatures (see at least, col. 1, lines 15-25: the examiner notes the use of digital signatures for a document which could be further used for client and server programs, col. 7, lines 35-49: the examiner notes the use digital signing of programs for authentication for additional security services by the policy server program, and col. 8, lines 45-50: the communication between client and server programs are signed).

Claims 13 and 40

Tumblin discloses in interprocess communications security system enabling secure trust relationships to be established at any level down to the level of individual application instances as executed on respective host computer systems interconnected by a communications network (see at least, abstract and col. 5, line 58 – col. 6, line 9: the

examiner notes communication policy and program policy) said system comprising: a) a first host computer operative to support execution of a first application instance within a first predefined process context (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the client program on the client); b) a second host computer system operative to support execution of a second application instance in a second predefined process context (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the server program on the server); c) control means, provided with respect to said first and second host computer systems, for establishing communications channels between said first and second host computer systems including a predetermined communications channel conducting communications between said first and second predefined process contexts, said control means being responsive to predetermined information identified with said first and second predefined process contexts to determine a session encryption key for use exclusively in encryption processing of communications conducted through said predetermined communications channel (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules

of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program)).

Claims 14 and 41

Tumblin discloses the interprocess communications security system of claim 13 wherein said predetermined information identified with said first and second predefined process contexts includes secure identifications of said first and second application instances (see at least, col. 5, lines 51-57: the examiner notes that each SPIM is linked to an SKI which is used as a secure identification for both client and server program).

Claims 15 and 42

Tumblin discloses the interprocess communications security system of claim 14 wherein said control means provides for a policy-based evaluation of said predetermined information identified with said first and second process contexts (see at least, col. 5, line 58 – col. 6, line 9: the examiner notes communication policy and program policy for both the client and server program and connection).

Claim 16

Tumblin discloses the interprocess communications security system of claim 15 wherein said first and second predefined process contexts are established on said first and second computer systems by first and second operating systems and wherein said control means includes policy enforcement means implemented in combination with said first and second operating systems to conditionally enable establishment of said predetermined communications channel subject to said policy-based evaluation (see at least, col. 6, lines 14-24).

Claim 17

Tumblin discloses the interprocess communications security system of claim 16 wherein said control means includes a security server computer system operable to receive said predetermined information, to perform said policy-based evaluation, and to control said policy enforcement means in conditionally enabling establishment of said predetermined communications channel (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program)).

Claim 18

Tumblin discloses the interprocess communications security system of claim 17 wherein said security server computer system determines said session encryption key (see at least, col. 9, lines 32-37).

Claim 19

Tumblin discloses the interprocess communications security system of claim 18 wherein said session encryption key is provided to said policy enforcement means to perform encryption processing for communications conducted between said first and second process contexts (see at least, col. 8, lines 45-49: the examiner notes further use of security measures (e.g. encryption, signing) and col. 9, lines 32-37).

Claim 20

Tumblin discloses the method of binding application execution contexts on network connected computer systems through a secure communications channel, said method comprising the steps of: a) first enabling execution of a first application instance on a first computer system dependent on a first security assessment of a first application context within which said first application instance is executable (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the client program on

the client); b) second enabling execution of a second application instance on a second computer system dependent on a second security assessment of a second application context within which said second application instance is executable (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the server program on the server); c) third enabling communications between said first and second application instances dependent on a mutual security assessment of said first and second application contexts; and d) selectively establishing an encrypted communications channel between said first and second application instances wherein use of said encrypted communications channel is enabled by a session key shared between said first and second application contexts (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program)).

Claim 21

Tumblin discloses the method of claim 20 wherein data, representative of said first and second application contexts, is communicated to a security server, said method further comprising the step of evaluating said data to perform said first, second, and mutual assessments of said first and second application contexts (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program)).

Claim 22

Tumblin discloses the method of claim 21 further comprising the step of determining, by said security server, said session key (see at least, col. 9, lines 32-37).

Claim 23

Tumbling discloses the method of claim 22 further comprising the step of communicating said session key from said security server to said first and second application contexts, wherein communications through said encrypted communications channel are transferred directly, relative to said security server, between said first and second application contexts (see at least, col. 8, lines 45-49: the examiner notes further

use of security measures (e.g. encryption, signing) and col. 9, lines 32-37: the examiner notes a session key provided encrypted secure communication).

Claims 24 and 30

Tumblin discloses the method of securely binding communications between processes, wherein application instances, within respective processes, are executed on computer systems in process execution contexts, said method comprising the steps of: a) intercepting communications between first and second predetermined process execution contexts; and b) encrypting intercepted network communication transmissions (see at least, col. 8, lines 45-48: the examiner notes further security measures (e.g. encryption, signing) and decrypting intercepted communication receptions utilizing an encryption key uniquely established based on an evaluation of authorization and authentication information descriptive of said first and second predetermined process execution contexts (see at least, col. 8, lines 45-48: the examiner notes further security measures (e.g. encryption, signing) and further if the transmission has been encrypted it must be decrypted (e.g. see at least, col. 1, lines 52-65: the examiner notes two keys have a mathematical relationship that if the first key is used for encrypting it can only be decrypted using the associated other key) and col. 9, lines 32-37:the examiner notes the use of session key for pre-established communication).

Claim 25

Tumblin discloses the method of claim 24 wherein sets of one or more related processes are executed in process execution contexts, and wherein said step of intercepting communications includes the steps of identifying said first and second predetermined process execution contexts as a unique communication session and of obtaining a session encryption key specific to said secure communications session for said network communication (see at least, col. 9, lines 32-37: the examiner notes the use of session key for pre-established communication) .

Claim 26

Tumblin discloses the method of claim 25 wherein said session encryption key is unique to said unique communications session (col. 9, lines 32-37:the examiner notes the use of session key for pre-established communication is based on a new session token which is unique for each client and server program communication).

Claim 27

Tumblin discloses the method of claim 26 further comprising the step of determining said session encryption key uniquely in connection with the establishment of said unique communications session (col. 9, lines 32-37:the examiner notes the use of session key for pre-established communication is based on a new session token which is unique for each client and server program communication).

Claim 28

Tumblin discloses the method of claim 27 further comprising the step of requesting, with respect to said first and second predetermined execution contexts, said session key from a security server (col. 9, lines 32-37:the examiner the security server program mutually authenticates and provides a session token which is used as the basis for the session key).

Claim 29

Tumblin discloses the method of claim 28 wherein said security server is an independent computer system relative to the computer systems providing for the execution of said first and second process execution contexts, wherein said step of requesting provides for the transfer of predetermined authorization and authentication information descriptive of said first and second execution contexts, including secure identifications of first and second application instances, to said security server, and wherein said security server performs said step of determining dependent on said predetermined authorization and authentication information (see at least, col. 5, line 58 – col 6, line 9 and FIG. 9: the security integration server).

Claim 31

Tumblin discloses the method of claim 30 wherein said step of intercepting is performed transparently with respect to said first and second application instances (see at least,

col. 8, lines 45-49: the examiner notes a communication policy could include extra encryption or signing which would be transparent to the client and server program).

Claim 32

Tumblin discloses the method of claim 31 further comprising the step of requesting said encryption key from a security server computer system separate from said first and second host computer systems, said step of requesting including the steps of communicating predetermined identification data, including an identification of said first and second application instances, to said security server computer system and of selectively receiving said encryption key (see at least, col. 7, lines 35-49 and col. 8, lines 45-49: the examiner notes a communication policy and program policy would include extra encryption or signing which is based off the SKI of the ASIM and NSIM of the client or server program).

Claim 33

Tumblin discloses the method of claim 32 further comprising the step of determining, by said security server computer system, said encryption key specific to said predetermined identification data (see at least, col. 7, lines 35-49 and col. 8, lines 45-49: the examiner notes a communication policy and program policy would include extra encryption or signing which is based off the SKI of the ASIM and NSIM of the client or server program).

Claim 34

Tumblin discloses a system of securing communications between application instances executable on respective host computer systems, said system comprising: a) first and second computer systems operable to execute respective pluralities of application instances (see at least, col. 3, lines 2-65: the examiner notes the use of security APIs for SKI management which are executed by an OS, col. 5, line 25-col. 6, line 10: the examiner notes the SIM link with an SKI that use the security APIs to access policy information regarding program policy on a security server, and col. 6, lines 14-24: the examiner notes the client/server program on the client/server and FIG. 2: the examiner notes a plurality of client/server programs); and b) first and second secure communications modules respectively executable by said first and second computer systems, said first and second secure communications modules being operative to identify discrete communications sessions between specific pairs of application instances among said pluralities of application instances and establish encrypted communications channels between said first and second secure communications modules for respective communication sessions (see at least, col. , line 58 – col. 6, line 10: the examiner notes a security integration server connected to the network and linked to the ASIM and NSIM modules of the client and server programs and col. 7, lines 50-65: the examiner notes a authenticating both the client and server programs via the use of SKI which link to policies on the security integration sever (e.g. which performs the mutual authentication via the policy information stored for both the client and server program))

Client 35

Tumblin discloses the system of claim 34 further comprising a security server computer system operative to provide a distinct session encryption key to said first and second secure communications modules for respective communication sessions (col. 9, lines 32-37: the examiner notes the use of session key for pre-established communication is based on a new session token which is unique for client program/server program)

Claim 36

Tumblin discloses the system of claim 35 wherein said security server computer system includes a policy database, wherein said first and second secure communications modules are coupleable to said security server computer system to provide predetermined request data with respect to a predetermined communication session, wherein said server computer system is operative to evaluate said predetermined request data against said policy database and selectively return said distinct session encryption key for said predetermined communication session (see at least, col. 5, line 58 – col. 6, line 9)

Claim 37

Tumblin discloses the system of claim 36 wherein said predetermined request data includes first request data including a first identification of a first application instance and second request data including a second identification of said second application instance (see at least, col. 6, lines 14-24)

Claim 38

Tumblin discloses the system of claim 37 wherein said first and second identifications are secure identifications (see at least, 52-57: the examiner notes that each SKI would be a secure identification for said first and second identifications)

Claim 39

Tumblin discloses the system of claim 38 wherein said predetermined request data identifies provides user identification, user authentication, and application instance identification information for said first and second application instances (see at least, col. 6, lines 24-30).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571)270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

/Kari L Schmidt/
Examiner, Art Unit 2139